

REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 USC § 102. Furthermore, the Applicants also submit that all of these claims now satisfy the requirements of 35 USC § 101 and 112. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 530-6671 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Title, specification and abstract amendments

As indicated above, the present specification is constituted by the amended sheets supplied with the Applicants' IPER. Given that the title as shown on the amended sheets differs from that shown on the filing receipt, the Applicants have now amended their title to conform it to that shown on the amended sheets.

The Examiner has pointed to an inadvertent error in the specification, specifically in row 6 (Step n = 6) of Table II the numeric string "5 5 6 3 5" should be "5 5 6 3 4". The Applicants have now appropriately corrected their specification.

Appl. No. 09/937,415
Amdt. dated June 6, 2005
Reply to Office Action of March 7, 2005

Additionally, various amendments have been made to the specification to correct minor inadvertent grammatical, idiomatic, spelling and formal errors, and to include appropriate section headings.

Lastly, the Examiner objected to the Applicants' abstract, as originally filed, owing to its inclusion of "input symbol (5,20)" and "function (2)" which the Examiner believes are not clearly defined. The Examiner has requested that the Applicants make appropriate corrections to the abstract and the specification. The Applicants have provided a replacement abstract which does not include any reference numbers, thus correcting this inadvertent error. Appropriate corrections have also been made to the present specification.

To expedite prosecution, the Applicants have enclosed: (a) a substitute specification which provides the specification contained in the amended sheets and incorporates with all the changes set forth above, and also (b) a marked-up specification which shows all these changes. None of these changes introduces any new matter into the application.

The Applicants now request that the Examiner enter the substitute specification.

Status of claims

To simplify amending the claims, the Applicants have now canceled claims 9-17 and replaced those claims with new claims 18-26. Not only do these new claims contain the

Appl. No. 09/937,415
Amdt. dated June 6, 2005
Reply to Office Action of March 7, 2005

substantive limitations of the prior claims but also contain various corrections and recitations that conform the former to the various dictates of US claim practice as well as provide appropriate clarifications.

Rejections

A. Rejection under 35 USC § 101

The Examiner has rejected claim 9 under the provisions of 35 USC § 101 as lacking utility.

Specifically, the Examiner stated that the subject matter then claimed was not technologically embodied but rather was just an abstract idea. The Examiner suggested that the Applicant incorporate the limitations in that claim as being embodied on a computer readable medium.

Independent claim 18, which corresponds to now canceled independent claim 9, is directed, pursuant to the Examiner's suggestion, to a computer readable medium.

Hence, this rejection is now overcome.

B. Rejection under 35 USC § 112

The Examiner has rejected claim 9 under the provisions of 35 USC § 112, first paragraph, as lacking enablement.

The Examiner states that the claim contains "subject matter which is not described in the specification

in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention." Specifically, the Examiner opines that a typical embodiment of an authentication system includes both enciphering and deciphering sections, though the latter is not clearly and specifically addressed in the specification.

Contrary to the Examiner's view, the application does address the need to have both enciphering and deciphering sections for authenticating the sender of a string of characters. In that regard, the Applicants point to page 1, lines 26-34 and page 1, line 39 - page 2, line 10 of their present specification which, with minor amendments, now state:

"In accordance with the present invention, the sender of the enciphered string of output characters and the receiver of the series must both dispose of the same key and the string of input characters used for enciphering, at any rate the portion of the latter series used for modifying the function. As a result, the method is particularly suited for authentication, the receiver of an enciphered string of characters being capable of checking whether a sender having an identity suggested to the receiver has utilized a corresponding key, and in the event of a positive outcome of that check, the identity of the sender is ensured to the receiver.

...

If the non-linear function used for enciphering were an invertible function, the receiver of the enciphered string of characters may carry out the check using the same function, the same key and the received string of characters as an input for the function. The result must be equal to the string of input characters used for enciphering. since the receiver may also carry out the check by executing the same operations as

the ones carried out by the sender, the series received by the receiver has to be equal to the series generated by the receiver. In such case, it is not required that the function be an invertible function, as a result of which, in the event of the complexity remaining constant, there may be realized a stronger enciphering function which is more resistant against attacks."

Any one of skill in the art will readily appreciate, from these passages, that the receiver of the enciphered characters, i.e. the ciphertext, contains a deciphering section that is either the same or complementary to the enciphering section present at the sending location. Inasmuch as the Applicants have fully described the enciphering section, those of skill fully understand that the deciphering section employs the same inventive methodology though in the same or an opposite manner -- depending on whether the enciphering function is invertible or not.

Therefore, the Examiner's view of the present specification is not correct.

Nevertheless, the present invention is directed to a method of enciphering that is used within the overall authentication process. Independent claim 18 is directed to this method, as implemented in executable instructions recorded on a computer readable medium. In that regard, the preamble of this claim recites:

"A computer readable medium containing computer executable instructions which ... authenticate a string having a plurality of input characters through use of a method which relies on an enciphering function that enciphers ... the string of input characters to yield a corresponding string having a plurality of output

Appl. No. 09/937,415
Amdt. dated June 6, 2005
Reply to Office Action of March 7, 2005

enciphered characters, the method comprising the steps of".

This method is described in full detail in the present specification to enable any one of skill to implement it within both an enciphering section and a deciphering section of a common system for authenticating a character string.

Accordingly, the Applicants submit that since the inventive method as recited in this claim is fully described and hence enabled by the specification, this claim meets the dictates of 35 USC § 112 and is patentable thereunder.

C. Rejection under 35 USC § 102

The Examiner has rejected claims 9-17, as they previously existed, under the provisions of 35 USC § 102 as being anticipated by the teachings of the Ritter '832 patent (United States patent 4,979,832 issued to T. F. Ritter on December 25, 1990). Inasmuch as claims 9-17 are now canceled, this rejection is moot. However, since these claims have been replaced by new claims 18-26, then to expedite prosecution, this rejection will be discussed in the context of these new claims and particularly with respect to new independent claim 18. In that context, this rejection is respectfully traversed.

The Ritter '832 patent is directed to a technique for enciphering data, which uses a substitution box. As described in this patent in col. 1, line 67 et seq., conventional encryption schemes at the time which relied on using substitution boxes, whether singly or multiple boxes used in some sequence (the latter being known as

"polyalphabetic" substitution ciphers), were relatively easy for cryptanalysts to penetrate owing to the fixed nature of the cipher, and also, where multiple substitution boxes were used, the fixed nature of the sequence of substitution boxes.

Another conventional approach relies, as discussed in col. 3, line 65 et esq. of the '832 Ritter patent and with specific reference to United States Patent 4,751,733, on using a substitution-permutation cipher where a sequence of substitutions and permutations is made to plaintext data, with each substitution being selected through use of a different key. Though the key, as disclosed in the '733 patent remains fixed during enciphering, the '832 patentee opines that even if the key were to so change, such as being "stepped" in some fashion or randomized, to provide increased enciphering complexity, the resulting cipher would still be vulnerable to cryptanalysis for the simple reason that the approach would still rely on selecting a static substitution table from amongst a fixed set of such tables. In that regard, col. 4, line 20 et esq. states:

"Because static pre-defined tables constitute the heart of this mechanism, it is essential that they be retained as secrets. Since the table contents do not change, they are amendable [sic] to cryptanalysis and eventual penetration."

Given this, one can reasonably infer from this conclusion that the '832 patentee would view any enciphering technique that relies on using pre-defined static substitution tables, in any manner, as insecure. This insecurity arises from the predictability of certain patterns appearing in the ciphertext, based on redundancies

and frequencies of occurrences, of expected letters in the plaintext. Fixed substitution ciphers do not change these frequencies of occurrence from the plaintext to the ciphertext..

To avoid the insecurity by substantially eliminating the predictability from the ciphertext while still using fixed substitution tables, the Ritter '832 patent teaches, to the extent relevant to the present invention, the concept of dynamically changing the substitution alphabets for each successive symbol in the plaintext. Specifically, after each symbol is enciphered, the substitution alphabet is changed for use in enciphering the next symbol in succession, and so on. As such, the substitution cipher is dynamically changed immediately before and for use with each and every successive plaintext symbol. See, e.g., col. 8, line 35 et esq. which generally describes this approach as:

"In the preferred embodiment, the just-used substitution value is exchanged with some value in the table selected by another data sequence; commonly, this other sequence will be pseudo-random."

As specifically described in col. 5, line 56 et esq. of this patent, two values, once combined, are used to control selection of the substitution alphabet to encrypt the next successive plaintext data symbol, and as more particularly discussed in col. 7, line 29 et esq., to change two substitution elements in the substitution box. One of these values is the incoming data symbol -- as symbolized by line 10 in FIG. 1; the other is a current value in a pseudo-random sequence -- as symbolized by line 16 in FIG. 1. The combination of these two values, as generated by

"Changes Controller" 18, and through application to Substitution Function F (shown as block 12 in FIG. 1), changes the substitution alphabet provided by this function. The resulting ciphertext symbol appears on output 14. The same exact pseudo-random string that is used to change the cipher for encryption must also be used to identically change the cipher for decryption and both pseudo-random strings must be used in a synchronized fashion. In that regard, the same pseudo-random value must be used to encrypt an input plaintext symbol and then decrypt the corresponding ciphertext symbol; otherwise, the decrypted ciphertext symbol will not identically match the input plaintext symbol and errors will arise.

Unfortunately, dynamically changing the substitution cipher for each and every symbol in a stream, as well as ensuring that the identical pseudo-random sequence is always used in a synchronized fashion for both encryption and decryption can entail, from a practical standpoint, lead to a fairly complex implementation. See page 2, lines 26-39 of the present specification where the '832 patent is discussed.

The present Applicants, who also rely on dynamically changing the substitution cipher, utilize a significantly different approach than that taught by the Ritter '832 patent.

Instead of repeatedly changing the substitution cipher for each and every successive input plaintext symbol, the Applicants' approach relies on modifying the encryption function, as an initial matter, before the encryption

process starts to yield a modified encryption function and then using the same modified function throughout an entire ensuing encryption process, such as to encipher symbols in a given input character string. The modification is not made in response to pseudo-random values, but rather through a string of modification characters which themselves are generated as a function of the plaintext data itself. The encryption function is also responsive to a string of key characters. For further details, in the context of a preferred embodiment, as to how the modification characters are generated and subsequently used to modify the encryption function, see, e.g., page 3, line 25 et seq. of the present specification.

The Applicants have advantageously found that the inventive approach provides sufficient robustness against cryptanalysis and hence added security over conventional approaches while eliminating the need for using synchronized pseudo-random sequences, thereby also affording a relatively simple implementation.

Nowhere does the '832 Ritter patent disclose, teach or even suggest, whether explicitly or implicitly, the inventive concept of modifying the substitution cipher, which is key-dependent, only once based on modification data, generated through use of the input plaintext data itself, and then using the same modified cipher, but without any further modification, throughout an ensuing encryption operation to encrypt a string of plaintext characters.

Moreover, if one skilled in the art, when faced with the problem that the present Applicants address --

namely using substitution ciphers in an authentication system but without employing synchronized pseudo-random strings, were to consider the '832 Ritter patent, that person would be led directly away from the present inventive approach. Why? Because since the same encryption function is used to encrypt an entire plaintext character string, regardless of the fact that that function was initially modified prior thereto (as the present Applicants now teach), the teachings of the '832 patent would view the modified encryption function as being fixed and hence too vulnerable to cryptanalysis.

Independent claim 18 contains suitable recitations directed to the distinguishing aspects of the present invention. Specifically, this claim recites as follows, with those recitations shown in a bolded typeface:

"A computer readable medium containing computer executable instructions which, when executed, authenticate a string having a plurality of input characters through use of a method which relies on an enciphering function that enciphers, in response to a string of key characters, the string of input characters to yield a corresponding string having a plurality of output enciphered characters, the method comprising the steps of:

modifying said enciphering function, by application of a modification function and in response to a string of modification characters; and

enciphering, by application of the enciphering function and in response to said string of key characters, said string of input characters so as to yield the corresponding string of output enciphered characters;

wherein:

said modification function is applied initially to said enciphering function, that is prior to the application of the enciphering function to generate all of the enciphered characters in the

corresponding string of output enciphered characters;
and

said modification function, once so initially applied, modifies the enciphering function in response to the modification characters, the modification characters being derived from said string of input characters." [emphasis added]

These distinguishing recitations of claim 18 are simply not identically disclosed, taught or even suggested - - whether implicitly or explicitly, by the teachings in the Ritter '832 patent.

Consequently, claim 18 is not anticipated by the teachings in this reference. Hence, this claim is patentable under the provisions of 35 USC § 102 over this reference.

Each of the pending claims 19-26 depends, either directly or indirectly, from claim 18 and recites further distinguishing features of the present invention.

Thus, each of these dependent claims is also not anticipated by the teachings of the Ritter '832 patent for the same exact reasons set forth above. As such, each of these claims is also patentable under the provisions of 35 USC § 102 over this reference.

Conclusion


Thus, the Applicants submit that none of the claims, presently in the application, is anticipated under the provisions of 35 USC § 102. Furthermore, the Applicants also submit that all of these claims now fully satisfy the requirements of 35 USC § 101 and 112.

Appl. No. 09/937,415
Amdt. dated June 6, 2005
Reply to Office Action of March 7, 2005

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,


June 6, 2005


Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & ASSOCIATES
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **June 7, 2005** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Mail Stop Amendment, Commissioner for Patents, Mail Stop Amendment, P.O. Box 1450, Alexandria, VA 22313-1450.


Signature

30,090
Reg. No.



Appl. No. 09/937,415
Amdt. dated June 6, 2005
Reply to Office Action of March 7, 2005
MARKED-UP SPECIFICATION

~~Method for authentication of a string of input characters.~~METHOD FOR
AUTHENTICATION OF A STRING OF INPUT CHARACTERS

Background of the Invention

5 1. Field of the Invention

The invention relates to a method ~~according to the preamble of claim~~
~~1 for use in authenticating an input character string.~~

2. Description of the Prior Art

10 A method of ~~said this~~ type is disclosed in EP-A-0399587. With the
known method, the function ("algorithm") applied for enciphering consists
of a non-linear function formed by a substitution box ("S box") generated
as a function of the key. The document '587 European patent application
provides no further description of the way in which the substitution box
is generated. For obtaining good statistical properties of the output of
15 the substitution box with respect to variable-~~import~~ input, a string of
characters obtained by applying the substitution box ~~are~~ is combined with
just as long a string of statistically well-distributed characters. The
string of characters obtained in this connection may be used for
20 enciphering a string of input characters to be enciphered ~~in~~ into an
enciphered string of output characters. By applying a key-dependent
substitution box instead of a permanent substitution box, the enciphering
function is reinforced.

25 An objection to the known method is that, when ~~there is the same key~~
~~is nearly substantially always used the same key, said always used,~~
reinforcement of the enciphering function in practice is appreciably
annihilated. Such may occur, e.g., upon authentication when using a chip
card, such as a calling card and a GSM card.

Summary of the Invention

30 The object of the invention is to exclude the drawbacks of the known
method. ~~To this end, the invention provides a method as described in~~
~~claim 1.~~

35 ~~The~~ In accordance with the present invention, the sender of the
enciphered string of output characters and the receiver of ~~said the~~ series
must both dispose of the same key and the string of input characters used
for enciphering, at any rate the portion of the latter series used for
modifying the function. As a result, the method is particularly suited
for authentication, the receiver of an enciphered string of characters
being capable of checking whether a sender having an identity suggested to

the receiver has ~~utilised~~utilized a corresponding key, and in the event of a positive outcome of ~~said-that~~ check, the identity of the sender is ensured to the receiver.

5 The string of characters used for modifying the function ~~are~~is particularly variable and ~~are~~is, e.g., a challenge number generated per session, any (different) number, or a variable attribute of the sender, such as a balance kept up to date on a chip card.

10 If the non-linear function used for enciphering were an invertible function, the receiver of the enciphered string of characters may carry out ~~said-the~~ check using the same function, the same key and the received string of characters as an input for the function. The result must be equal to the string of input characters used for enciphering. Since the receiver may also carry out the check by executing the same operations as the ones carried out by the sender, the series received by
15 the receiver ~~having~~has to be equal to the series generated by the receiver. In such case, it is not required that the function be an invertible function, as a result of which, in the event of the complexity remaining constant, there may be ~~realised~~realized a stronger enciphering function which is more resistant against attacks.

20 The function applied to enciphering preferably is a non-linear function which may be formed by way of a substitution box or a cryptographic function, such as a function in which, depending on the input and the key, specific operations are carried out or not.

25 It is noted that EP0801477 discloses an encryption method in which an "internal state" is controlling an encryption function which h, in each encryption round, modifies the encryption function. According to the present invention, the encryption function is modified only once, in an initial step, while always, after the initial modification, the same encryption function is used in every new encryption round. Contrary to
30 that, in the known method the encryption function is modified in every encryption round. Further, in the known method the encrypting function is not modified on the basis of the input txt. According to the present ~~invention-invention~~ the input text forms an essential parameter in modifying the encryption function.

35 Next, it is noted that US4979832 discloses an enciphering method in which a pseudo-random input string is added to an encryption function. The pseudo-random string used in the encryption function also has to be available in the decryption process. In the known method the encryption function is dynamically (continuously) modified, during the encryption
40 processes. This is essential in ~~the method according that method~~

otherwise the system would be highly insecure. According to the present invention, however, there is only an initial modification of the encryption function, prior to the encryption process itself.

Consequently, during the subsequent encryption process the encryption function is not changed any more. The known method is aimed at encryption/decryption. The method according to the invention is specifically designed for authentication and even can in practice not be used for encryption/decryption.

Brief Description of the Drawings

Further properties and advantages of the invention will become clear from the explanation following below of embodiments of the invention in conjunction with the enclosed drawings, in which:

FIG. 1 shows a diagram of a known enciphering function;

FIG. 2 shows a diagram of a first embodiment of the invention;

FIG. 3 shows a flow diagram for the operation of the embodiment according to FIG. 2; and

FIG. 4 shows a ~~different~~second embodiment of the invention.

Detailed Description

By way of a block 1, FIG. 1 presents a known enciphering function (or encryption function). The enciphering function ~~utilises~~utilizes one or more functions 2, also presented by blocks. Assuming a string of input characters IN on line 3 to be enciphered, the enciphering function using a secret key 4 determines an enciphered string of output characters EXIT on line 5. The known enciphering function DES [= Data Encryption Standard] operates according to said principle, eight non-linear functions being used which are formed by substitution boxes ("S boxes"). The invention is not limited, however, to the DES function; neither is it limited to using non-linear functions and substitution boxes for the functions.

FIG. 2 shows a diagram of an enciphering function (denoted as enciphering algorithm) 7 based on the enciphering function of FIG. 1, but according to the invention. The functions are indicated by reference numeral 8. The functions 8 may be modified by applying ~~an associated~~reference function associated modification functions (denoted as modification algorithms) 9 based on the string of input characters IN on line 3 or part thereof. The modification functions 9 need not be equal.

Below, the operation of the enciphering function of FIG. 2 will be explained with reference to the flow diagram of FIG. 3.

A modification function 9 modifies the function 8 based on a string of modification characters initially derived from the string of input characters IN 3—(block 11). Modifying the function 8 takes place in several

steps, namely, the steps $n=0$ to $n=N_{\max}$ inclusive, N_{\max} being permitted to be permanent or also depending on, e.g., the series IN-3. That is why, at the start of the modification of the function 8, a step counter is reset (block 12). Subsequently, the function 8 is modified, based on the value of n and the modification series (block 13). Then the number of steps counted is incremented by 1 (block 14). Subsequently, it is checked whether the function 8 has already been modified the maximum number of times (block 15). When this condition is met, the modification of the function 8 is terminated; otherwise the string of modification characters are modified (step 16) and the function 8 is modified once again based on the new value of n and the modified string of modification characters (step 13). In Box I following below, an example is given for the operation of the enciphering function 7 shown in FIG. 2.

TABLE I

Step n	String of modification characters for n>0 x(2) := (x(0) + x(1))mod8			From step n=0, exchange y(nmod8) and y(x(0))								
	x(0)	x(1)	x(2)	i y(i)	0	1	2	3	4	5	6	7
0	5	2	3		<u>4</u>	0	5	7	6	<u>3</u>	1	2
1	2	3	7		4	<u>5</u>	<u>0</u>	7	6	3	1	2
2	3	7	5		4	5	<u>7</u>	<u>0</u>	6	3	1	2
3	7	5	2		4	5	7	<u>2</u>	6	3	1	<u>0</u>
4	5	2	4		4	5	7	2	<u>3</u>	<u>6</u>	1	0
5	2	4	7		4	5	<u>6</u>	2	3	<u>7</u>	1	0
6	4	7	6		4	5	6	2	<u>1</u>	7	<u>3</u>	0
7	7	6	3		4	5	6	2	1	7	3	<u>0</u>
8	6	3	5		<u>1</u>	5	6	2	<u>4</u>	7	3	0
9	3	5	1		1	<u>2</u>	6	<u>5</u>	4	7	3	0

It is assumed that the set of characters comprises eight characters, shown in the Table with the numerals 0 to 7 inclusive. It is further assumed that the function 8 is formed by a substitution box. ~~Said~~ ~~This~~ box may be ~~realised~~ realized by a rewritable memory having eight memory locations containing addresses or sequential numbers $1=0 \dots 7$. The memory locations each comprise one of the characters, each character figuring only once in the memory locations. In Table I, the content of a memory location having

address or sequential number i is indicated by $y(i)$. Initially, the memory locations for $i=0\dots 7$ contain the characters 3, 0, 5, 7, 6, 4, 1, 2, respectively. ~~Said-This~~ string of characters ~~form-forms~~ an initial substitution box. A character of a string of characters to be enciphered is considered to be address or sequential number i , and is replaced by the character in the memory location having ~~said-that~~ address. According to the initial substitution box of Table I, e.g., 0 is therefore replaced by 3, 1 by 0, 2 by 5, ..., 7 by 2.

Before a string of characters to be enciphered ~~are-is~~ actually enciphered, according to the invention the initial substitution box is modified first. According to the example of Table I, modification takes place in ten steps (step $n=0$ to $n=N_{\max}$ inclusive). The modification takes place depending on the characters of the string of characters to be enciphered, at any rate of several characters thereof. In Table I, the characters to be enciphered which are used for the modification of the substitution box are the characters 5, 2 and 3 indicated at step $n=0$. ~~Said-These~~ characters are allotted to variables $x(0)$, $x(1)$ and $x(2)$, respectively.

During the first step with $n=0$, the character $y(n)$, i.e., the character 3 of memory location 0, is exchanged with the character $y(x(0))$, namely, character 4 of location $x(0)=5$. In Table I, for clarity's sake, the exchanged characters of the substitution box of eight characters are underlined for each of the ten steps $n=0, \dots, 9$.

Subsequently, there is calculated an auxiliary variable h , which is equal to:

$$h = (x(0) + x(1)) \text{ modulo (the number of possible characters),}$$

or in the example

$$h = (x(0) + x(1)) \text{ modulo } 8.$$

Subsequently, the characters of the string of modification characters $x(0)$, $x(1)$ and $x(2)$ are replaced as follows (" $:=$ " means "becomes", i.e., an allotment).

$$x(0) := x(1),$$

$$x(1) := x(2), \text{ and}$$

$$x(2) := h.$$

For each step, modifying characters based on the step number and the characters of the string of modification characters are repeated a suitable number of times, in the example of Table I $N_{\max}+1=10$ times. At the end of said modification character, the initial substitution box:

3, 0, 5, 7, 6, 4, 1, 2

has been replaced by a final substitution box:

1, 2, 6, 5, 4, 7, 3, 0.

Subsequently, the characters of an input series to be enciphered may, according to the order of the characters in the eventual substitution box, be replaced for providing an output string of enciphered characters.

5 As a result, in the example the string of input characters 5, 2, 3 are replaced by 7, 6, 5, respectively. Said string of output characters are used for possible further steps of the enciphering character.

10 FIG. 4 shows the diagram of an enciphering function (also denoted as enciphering algorithm) 18 which differs from the enciphering function 5-7 of FIG. 2 in that the modification function 9 is replaced by a modification function (denoted as modification algorithm) 19. Just as the modification function 9, the modification function 19 depends on a number of characters IN 3-to be enciphered, but in addition on a number of characters of the key on line 4.

15 Table II offers an example of the operation of the modification function 19.

TABLE II

Step n	String of modification characters for n>0 <u>x(2):=(x(0) + x(1))mod8</u>					From step n=0, exchange y(nmod8) and y(x(0))								
	x(0)	x(2)	x(4)			i	0	1	2	3	4	5	6	7
	x(1)	x(3)				y(i)	3	0	5	7	6	4	1	2
0	5	2	3	2	4		<u>4</u>	0	5	7	6	<u>3</u>	1	2
1	2	3	2	4	7		4	<u>5</u>	<u>0</u>	7	6	3	1	2
2	3	2	4	7	5		4	5	<u>7</u>	<u>0</u>	6	3	1	2
3	2	4	7	5	5		4	5	<u>0</u>	<u>7</u>	6	3	1	2
4	4	7	5	5	6		4	5	0	7	<u>6</u>	3	1	2
5	7	5	5	6	3		4	5	0	7	6	<u>2</u>	1	<u>3</u>
6	5	5	6	3	5 <u>4</u>		4	5	0	7	6	<u>1</u>	<u>2</u>	3
7	5	6	3	5	2		4	5	0	7	6	<u>3</u>	<u>2</u>	<u>1</u>
8	6	3	5	2	3		<u>2</u>	5	0	7	6	3	<u>4</u>	1
9	3	5	2	3	1		2	<u>7</u>	0	<u>5</u>	6	3	4	1

20 Table II differs from Table I only in that the string of modification characters $x(0)$, $x(1)$, $x(2)$ are completed by $x(3)$, $x(4)$. The characters $x(3)$ and $x(4)$ are derived from the key 4. In the example of

Table II, the initial string of modification characters is 5, 2, 3, 2, 4. According to Table II, the eventual substitution box is:

2, 7, 0, 5, 6, 3, 4, 1.

5 The string of input characters IN 3—having the characters 5, 2, 3 is replaced, according to said eventual substitution box, by the enciphered string of output characters EXIT on line 20 having the characters 3, 0, 5.

10 The characters of the initial substitution box may be sorted at random for as long as both the sender of a string of enciphered characters ~~UIT-5~~ (see FIG. 1) and the receiver of the string of enciphered characters use the same initial substitution box. If it is possible to always meet ~~said this~~ condition, the enciphering function may be reinforced by using, as an initial substitution box, a substitution box used during a preceding enciphering process, e.g., the most recently used eventual substitution box. If there is a danger that ~~said this~~ condition is not always met, it
15 may be provided that the receiver of the string of enciphered characters 5 recalls several of such preceding substitution boxes and uses an older one thereof if deciphering the series received leads to a negative check result.

20 Since, both during enciphering a string of characters and during deciphering thereof, the keys used must be equal and knowledge must be available on the string of input enciphered characters—~~IN-3~~, the receiver of the enciphered series may carry out exactly the same operation, i.e., enciphering, as the receiver has carried out, and compare the results to one another. In this event, a non-invertible function may be used for the
25 function which, in the event of constant complexity, makes a stronger enciphering function possible.

The modification functions explained in conjunction with Tables I and II serve only as an example. For modifying the string of modification characters there may be applied, e.g., for each step, more than two and/or
30 a different number of modulo additions, and the characters of the modification series may be rearranged in other ways instead of by way of simple shifting.